

#3

1/21

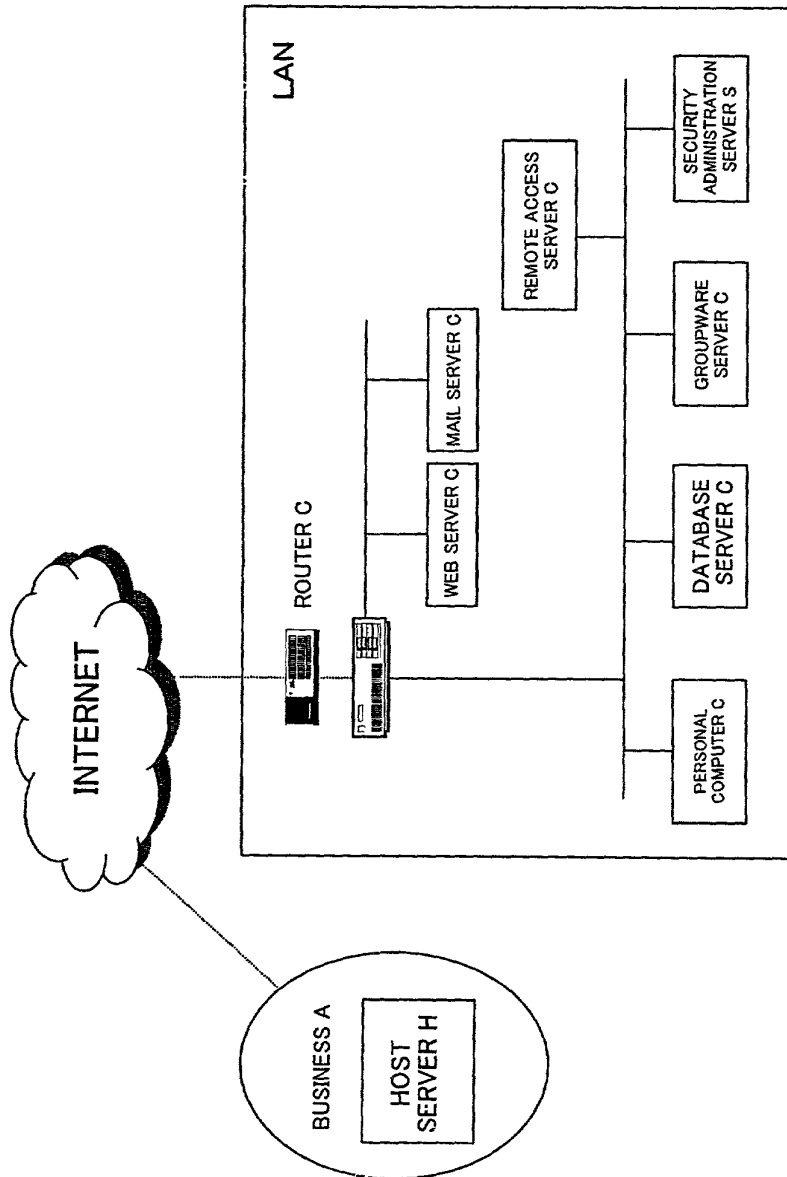


FIG. 1

2/21

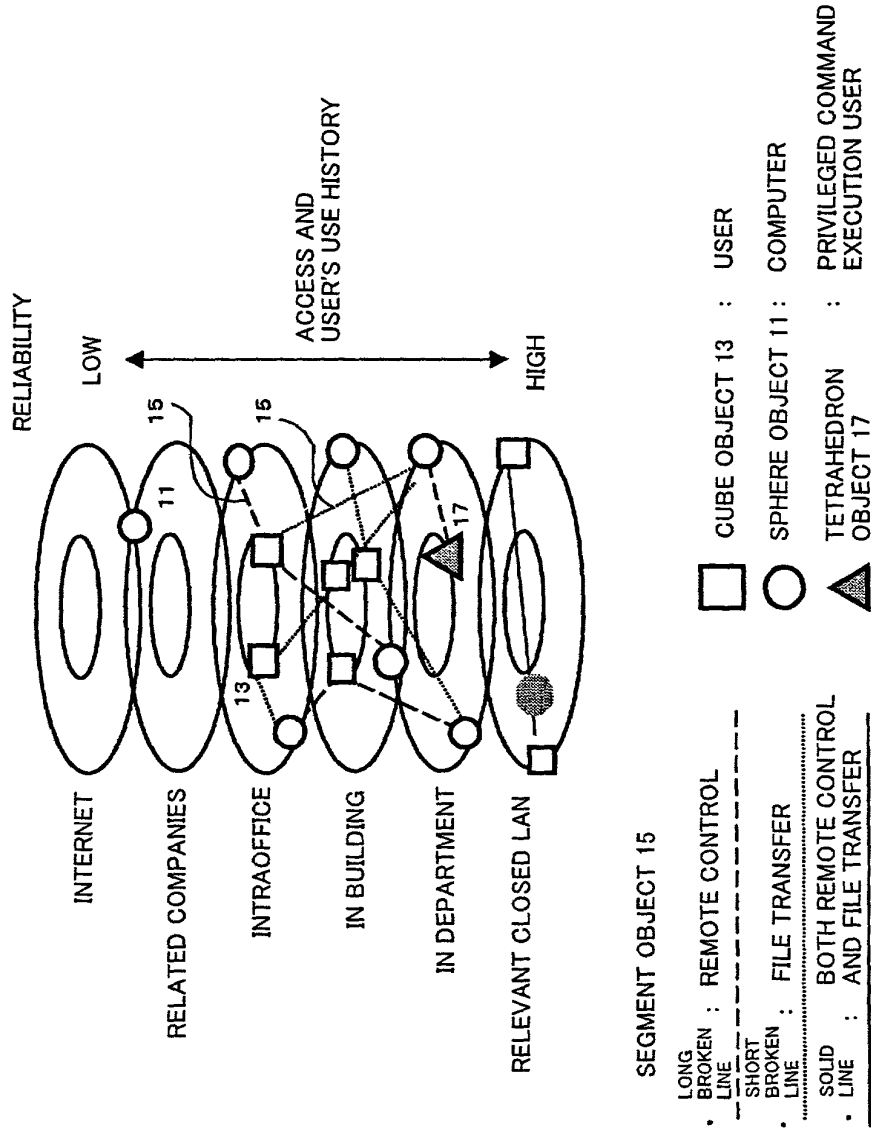


FIG. 2

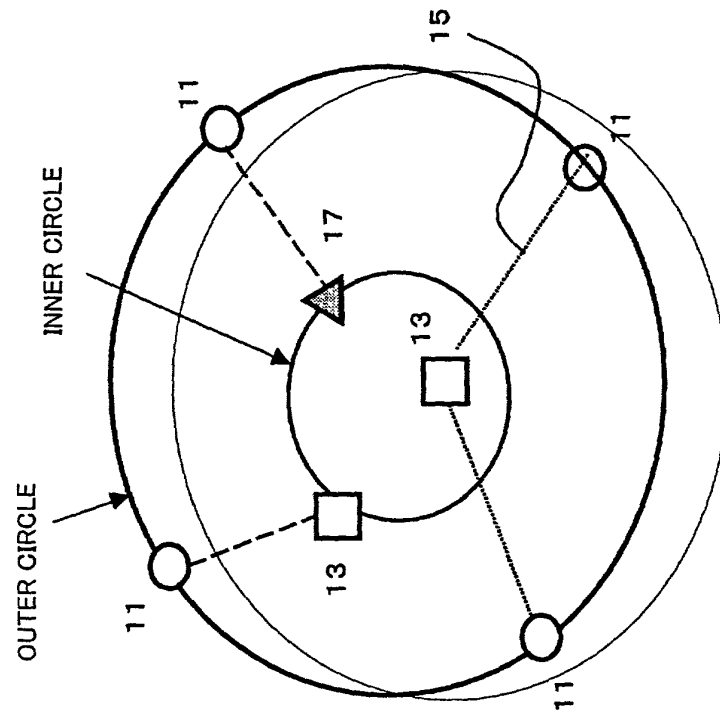


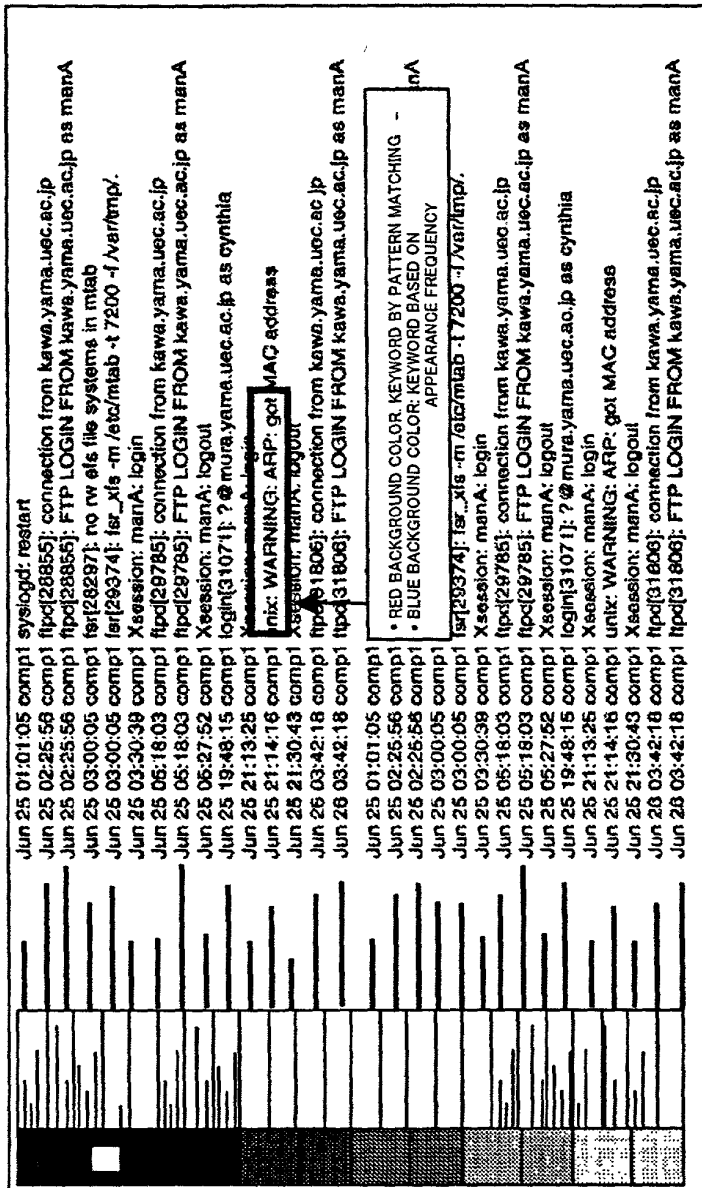
FIG. 3

4/21

DEVICE TO BE MONITORED	DISPLAY METHOD OF LAYERS (GROUP CLASSIFICATION)					DISPLAY TIME		OPERATION OF DISPLAY ANGLE	
	FOR EACH DOMAIN	FOR EACH DEPARTMENT	FOR EACH BUILDING FLOOR	FOR EACH ACCESS TYPE		REAL TIME	PLAYBACK	DEFAULT	ARBITRARY
1 PERSONAL COMPUTER			○			○			○
2 DATA BASE SERVER				○		○			○
3 WEB SERVER	○					○		○	
4 MAIL SERVER		○					○	○	
5									
6									
7									
8									
9									
10									
SETTING ENVIRONMENT	OS					DHCP ENVIRONMENT		LOG COLLECTION TIME	
	unix	unix	unix	Windows		OPEN	SEER DHCP	5 MINS.	ARBITRARY
1 PERSONAL COMPUTER	○						○	○	
2 DATA BASE SERVER	○						○	○	
3 WEB SERVER			○			○		○	
4 MAIL SERVER			○			○			240MINS
5									
6									
7									
8									
9									
10									

FIG. 4

5/21



24

23

21

22

FIG. 5

**FIG. 6**

**FIG. 6**

7/21

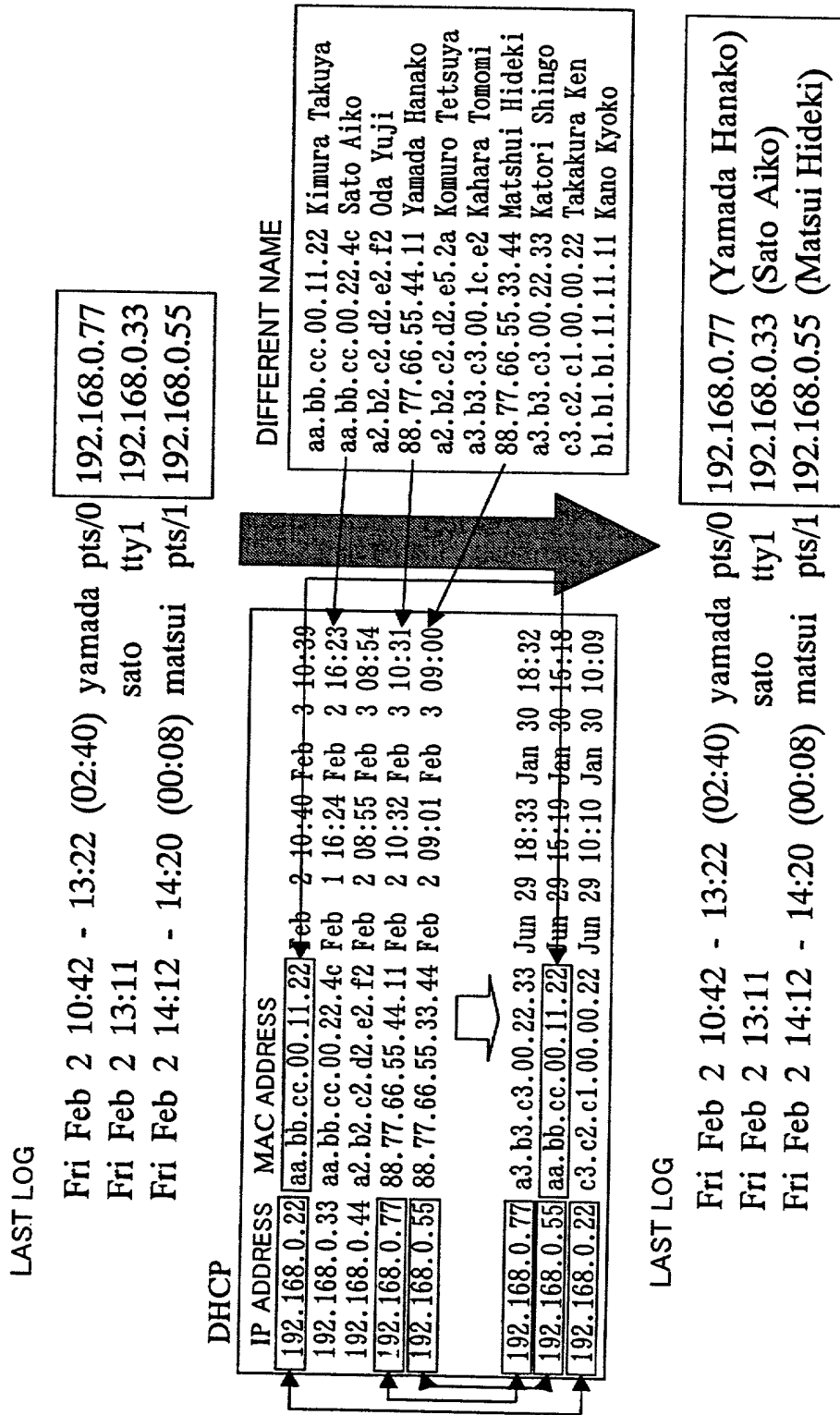


FIG. 7

8/21

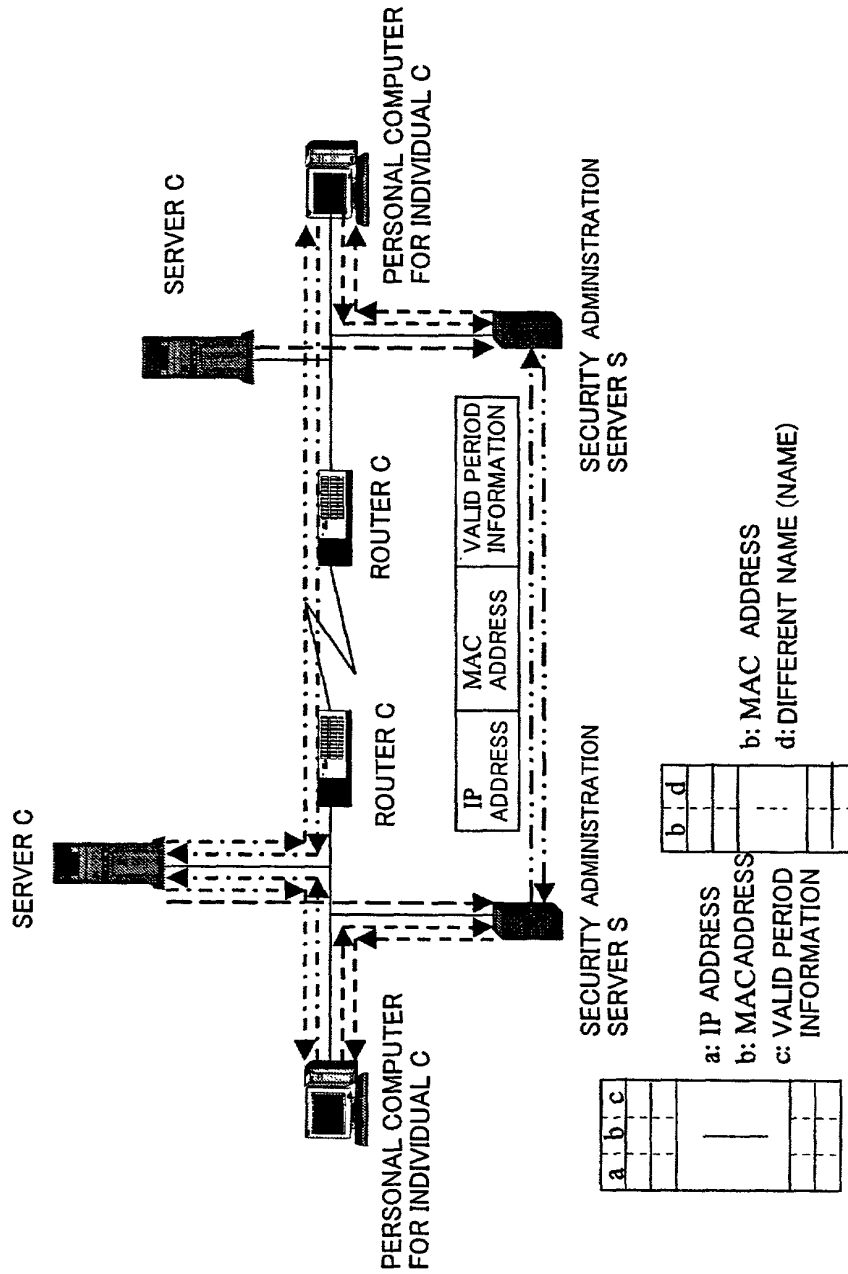


FIG. 8

9/21

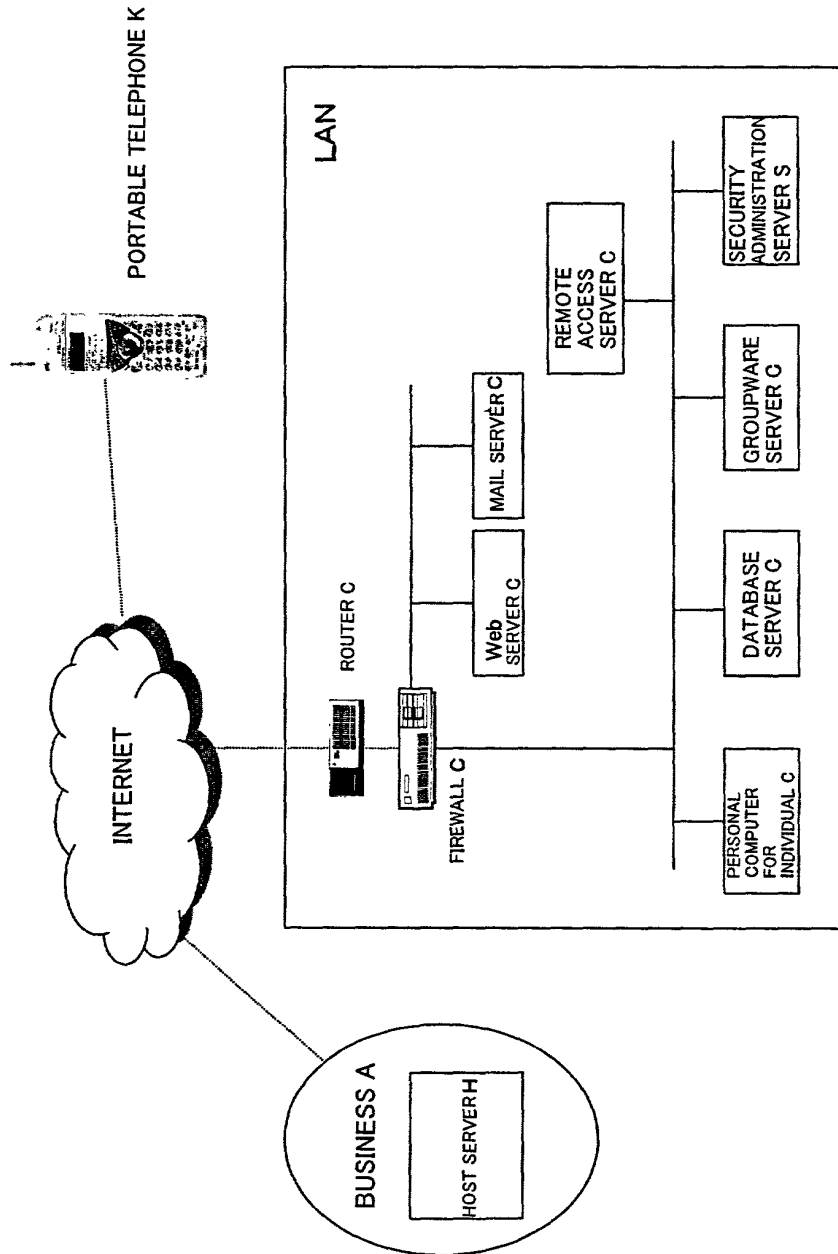


FIG. 9

10/21

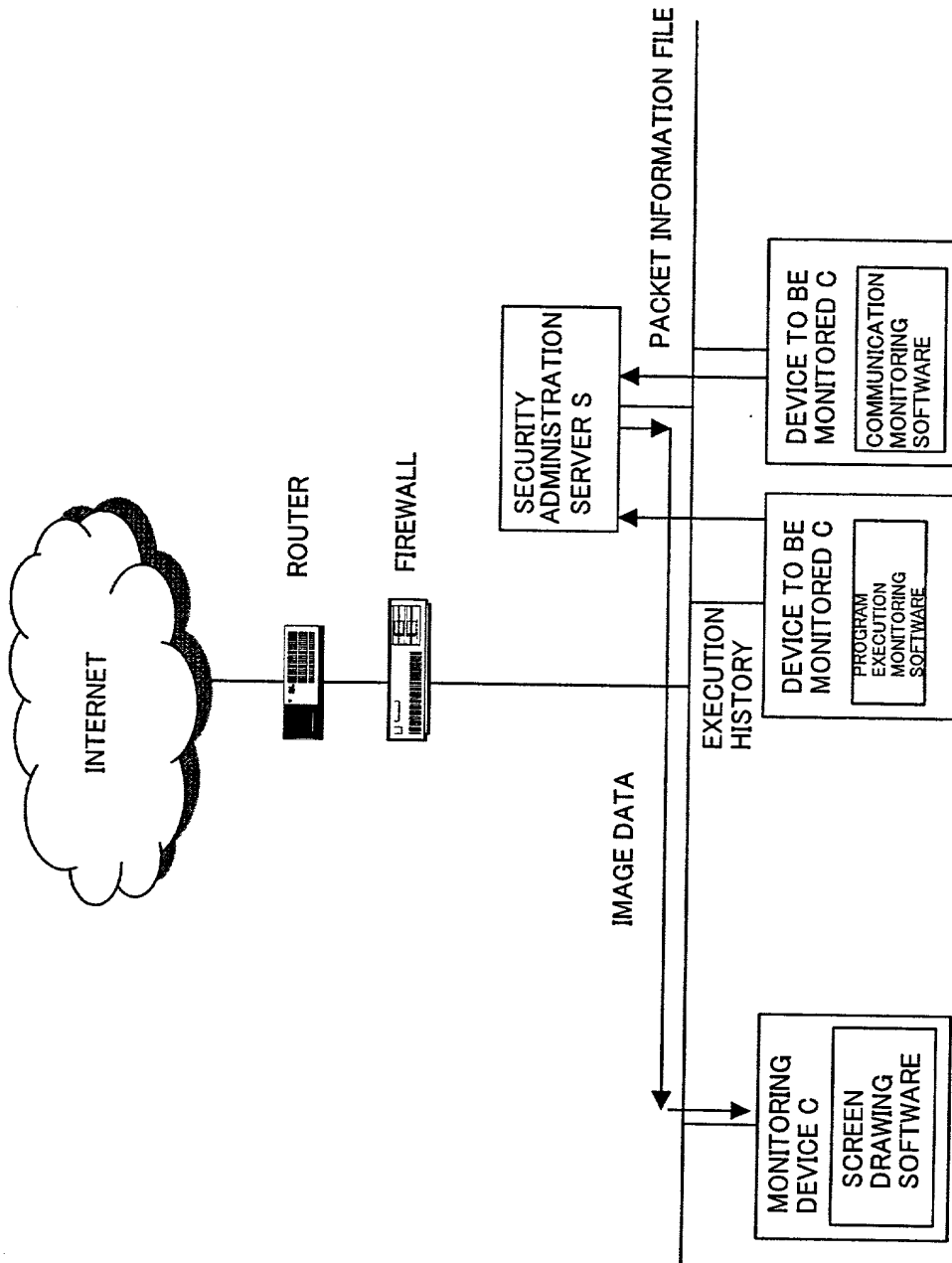
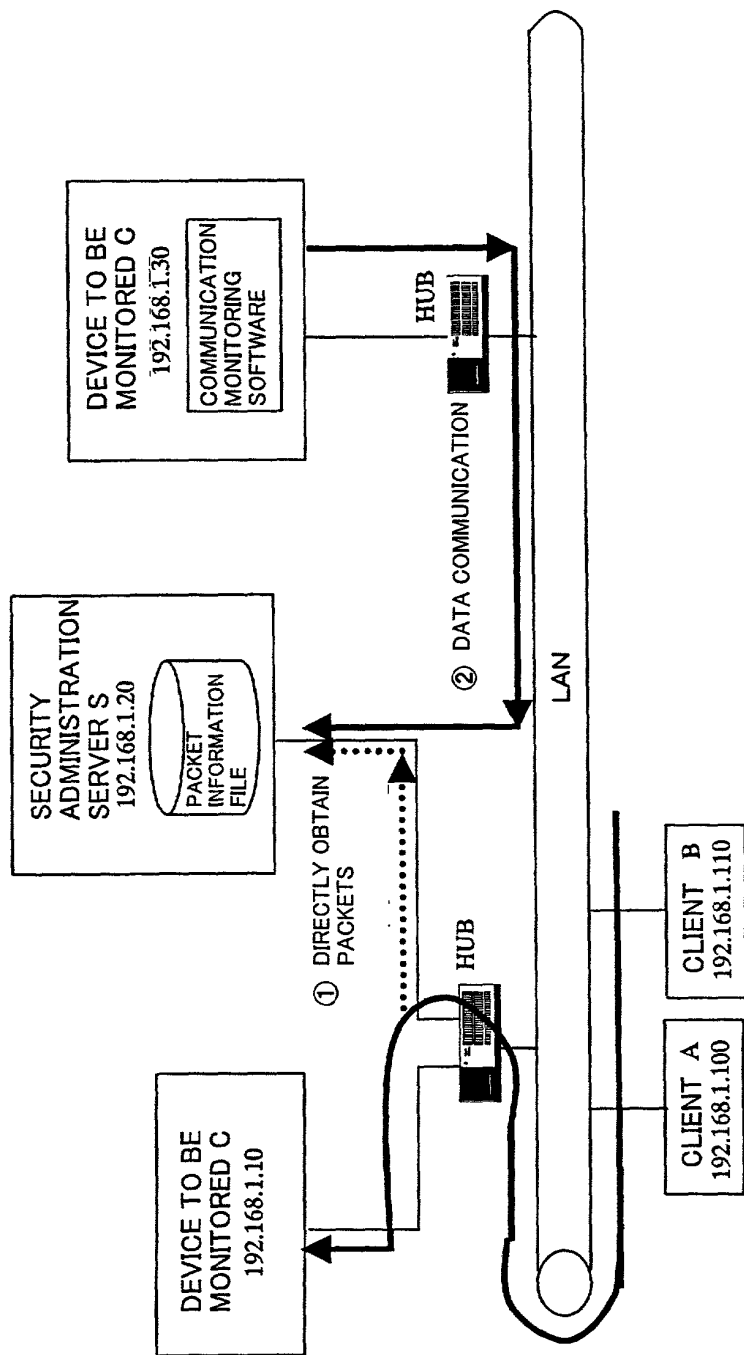


FIG. 10

11/21



- ① COMMUNICATION PACKETS OF DEVICE TO BE MONITORED C CONNECTED TO THE SAME HUB AS SECURITY ADMINISTRATION SERVER S ARE DIRECTLY OBTAINABLE
- ② COMMUNICATION PACKETS OF DEVICE TO BE MONITORED C CONNECTED TO A DIFFERENT HUB THAN SECURITY ADMINISTRATION SERVER S, ARE ACCUMULATED AND STORED AT DEVICE TO BE MONITORED C SIDE, AND CONCENTRATED SUITABLY TO SECURITY ADMINISTRATION SERVER S BY DATA COMMUNICATION VIA LAN.

FIG. 11

12/21

DATA FORMAT OF PACKET INFORMATION FILE

FIELD NAME	DESCRIPTION
time	COLLECTION TIME (SERVER TIME)
btFlags	0:IN 1:OUT (FROM SERVER) 2:SMB (SUCH AS COMMON FILE ACCESS)
wLength	ORIGINAL LENGTH OF PACKET
mwMac	CLIENT MAC ADDRESS
dwIPAddr	CLIENT IP ADDRESS
wPort	SERVER PORT NUMBER
btDataLength	LENGTH OF PORTION OF VARIABLE DATA OF PACKET (0 TO 255)
btData[256]	VARIABLE DATA OF 256 PACKETS (VARIABLE LENGTH)

FIG. 12

BASIC VISUALIZATION DATA

FIELD NAME	DESCRIPTION
time	COLLECTING TIME (TIME AT SECURITY ADMINISTRATION SERVER)
wServerID	IDENTIFIER OF SERVER TO BE MONITORED
wType	TYPE OF PACKET (01:Login...65:Mail...)
mwMac	CLIENT MAC ADDRESS
dwIPAddr	CLIENT IP ADDRESS
wOriginalLength	ORIGINAL LENGTH OF PACKET
btData[256]	CHARACTER DATA FOR EACH TYPE OF 256 PACKETS (Login:UserID/Mail:from.to...)

FIG. 13

13/21

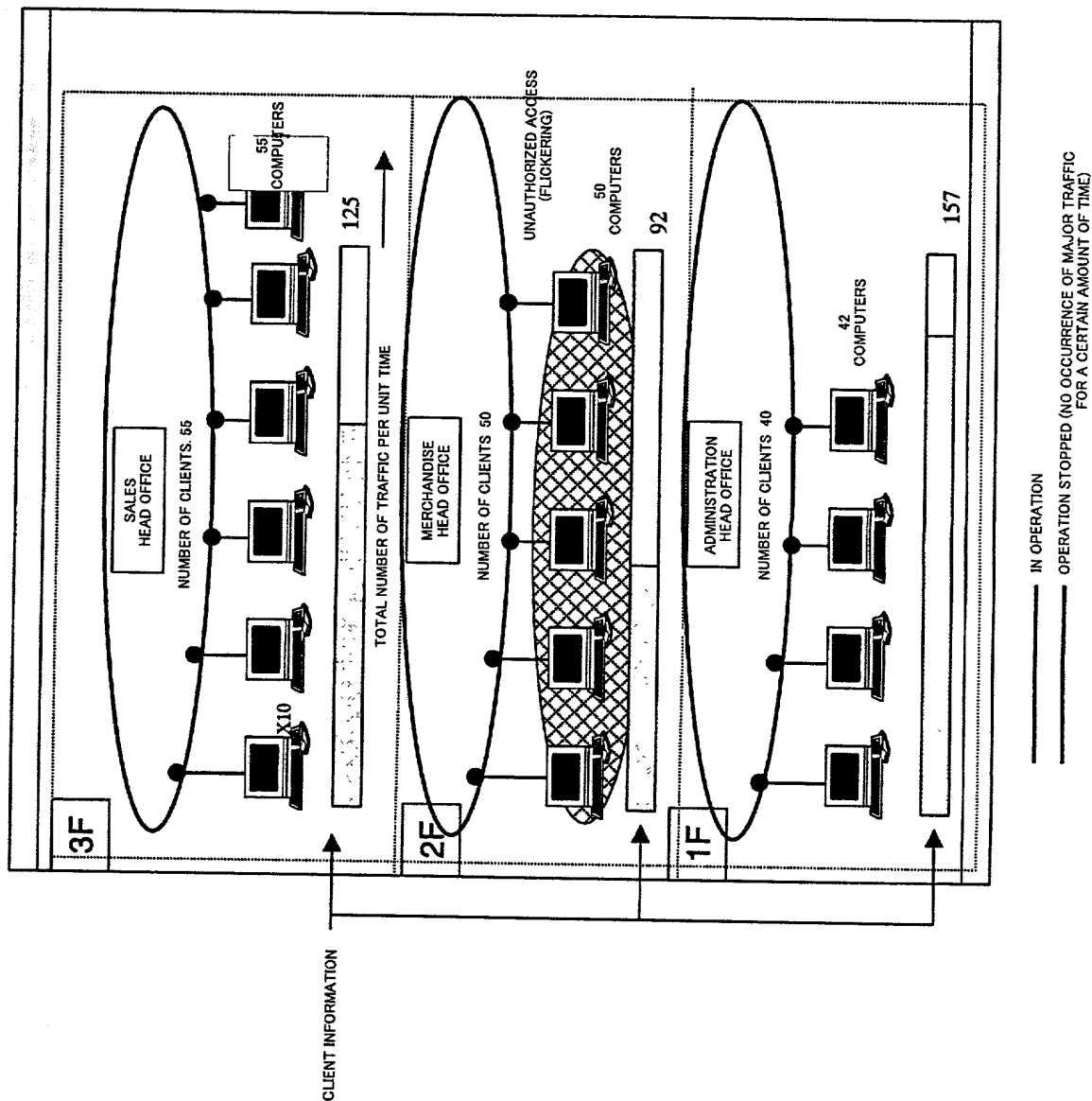


FIG. 14

14/21

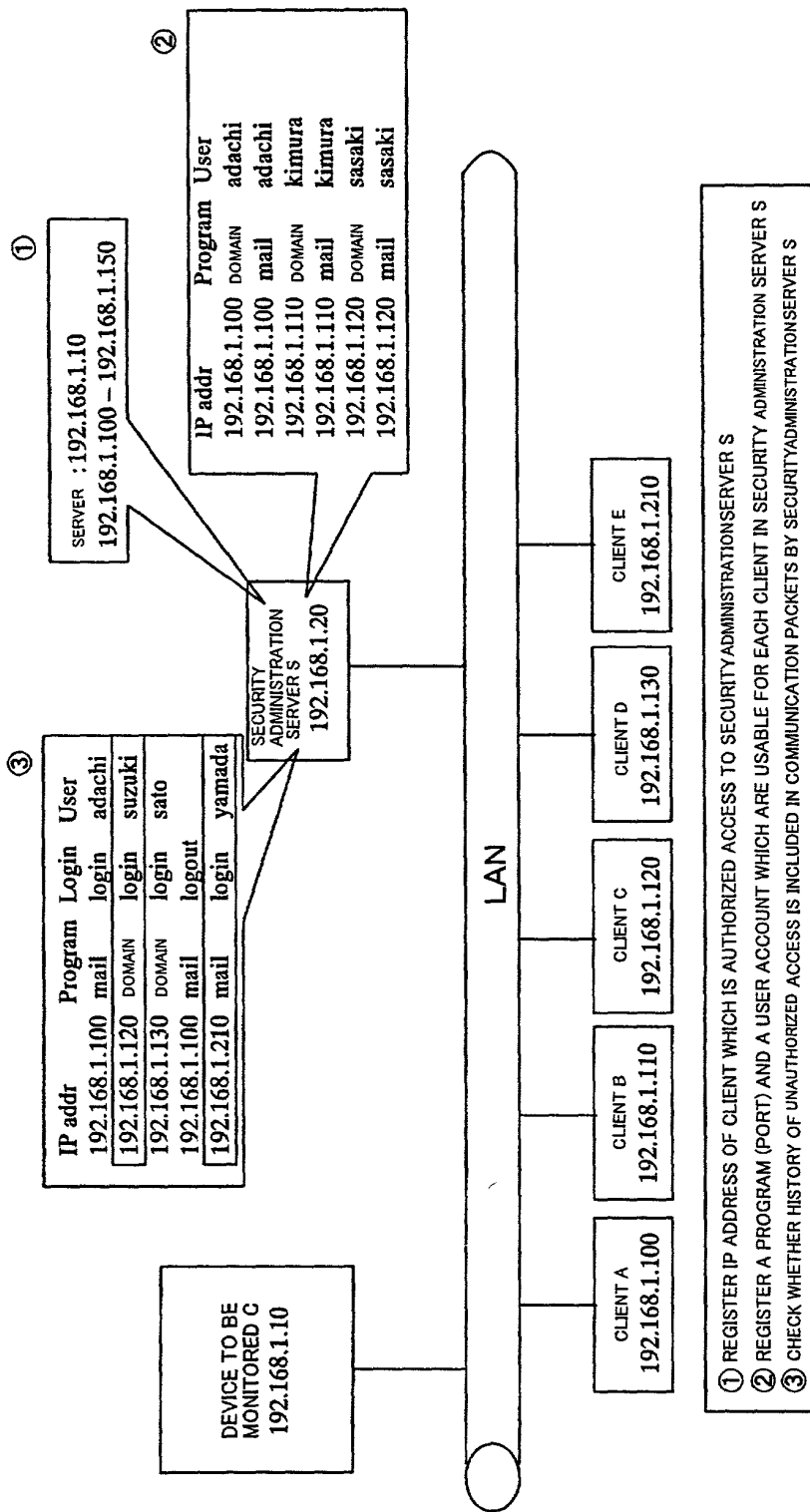


FIG. 15

15/21

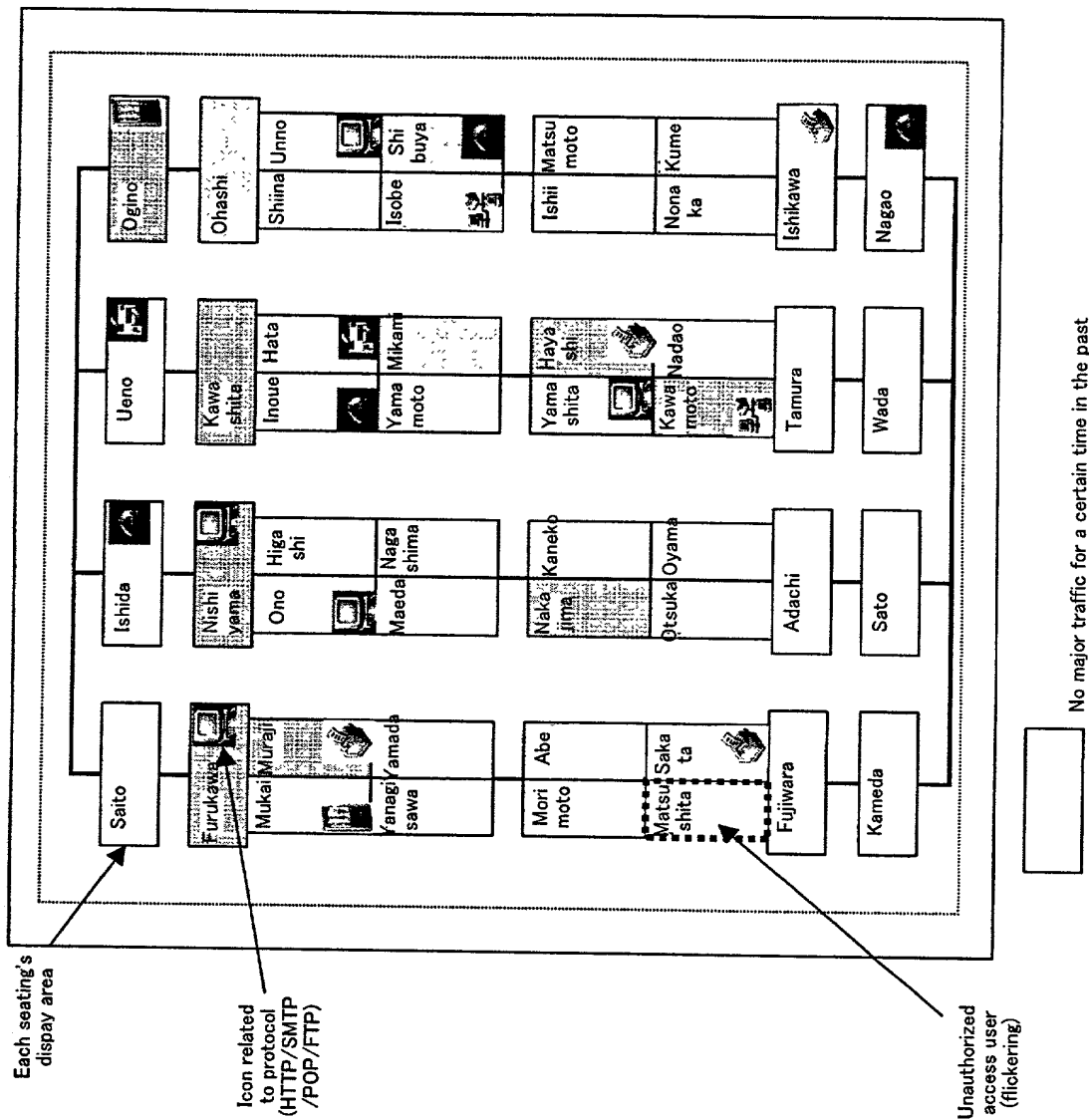


FIG. 16

16/21

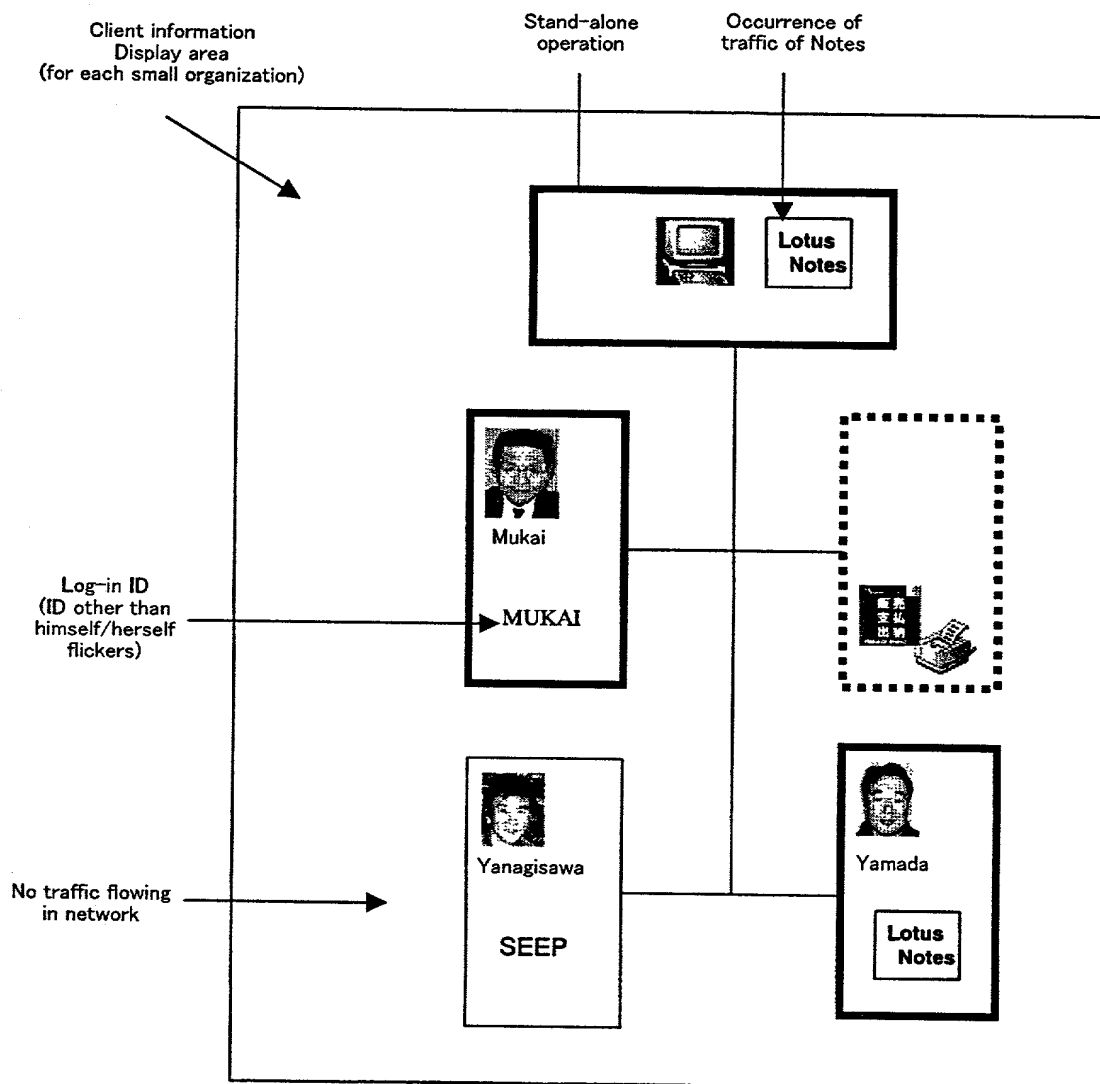


FIG. 17

17/21

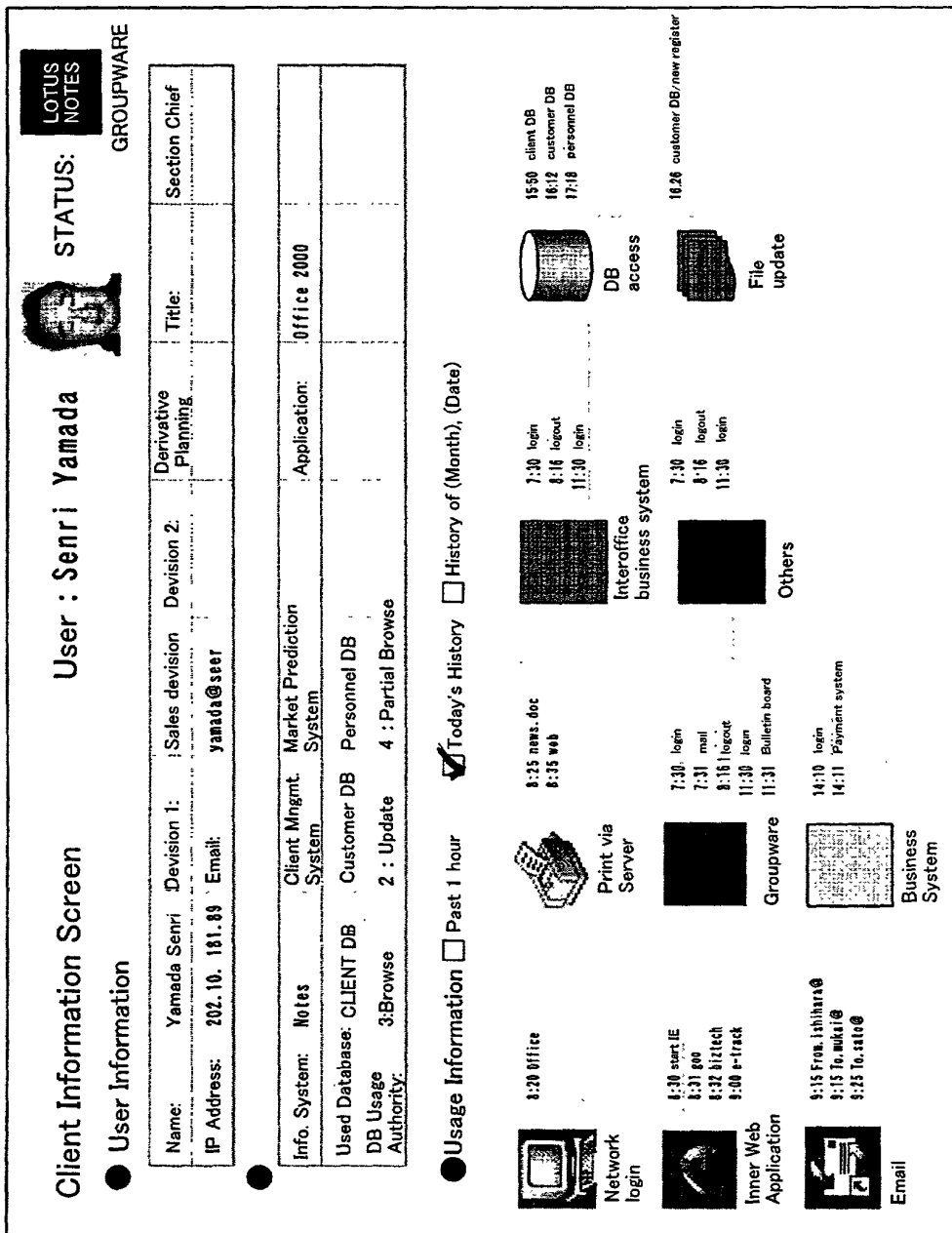


FIG. 18

18/21

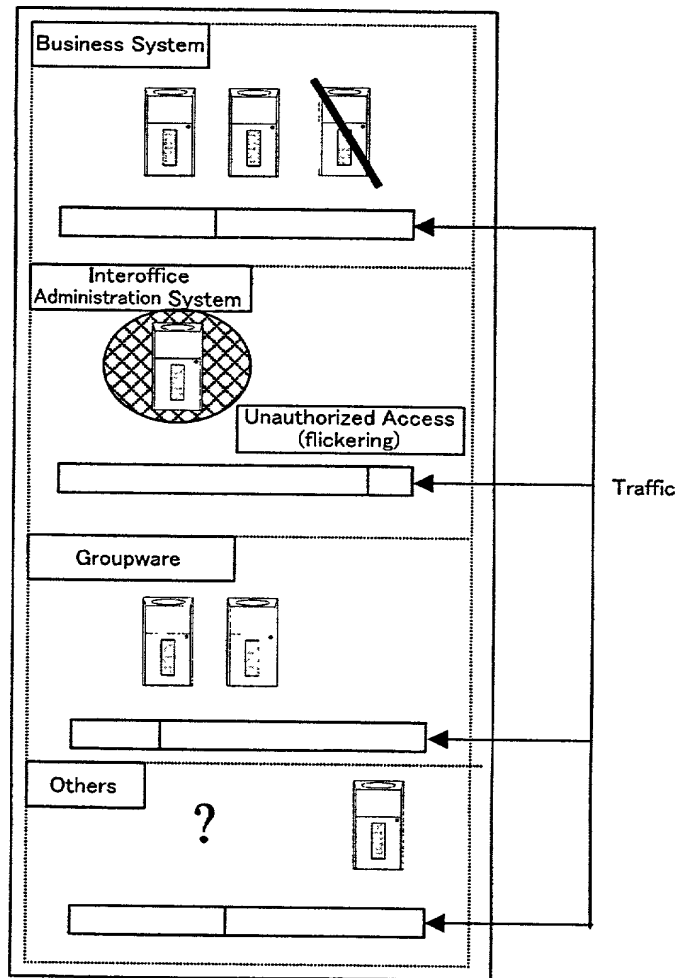


FIG. 19

19/21

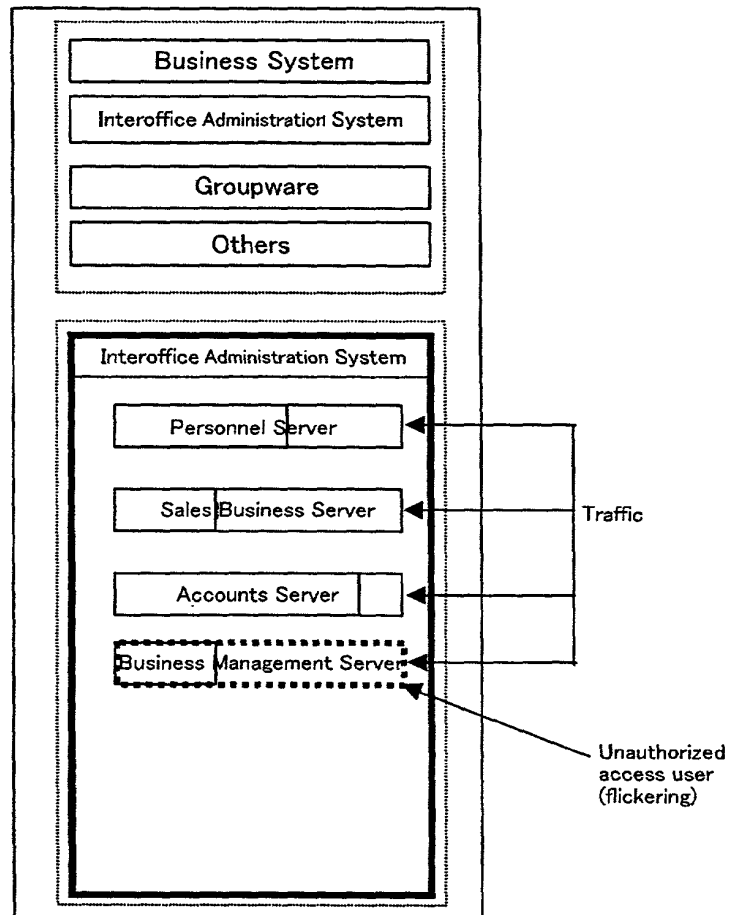


FIG. 20

20/21

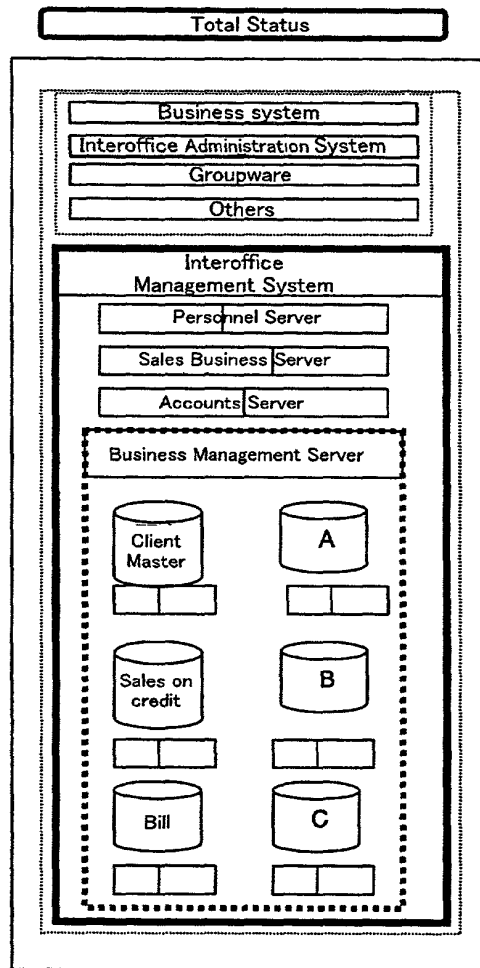


FIG. 21

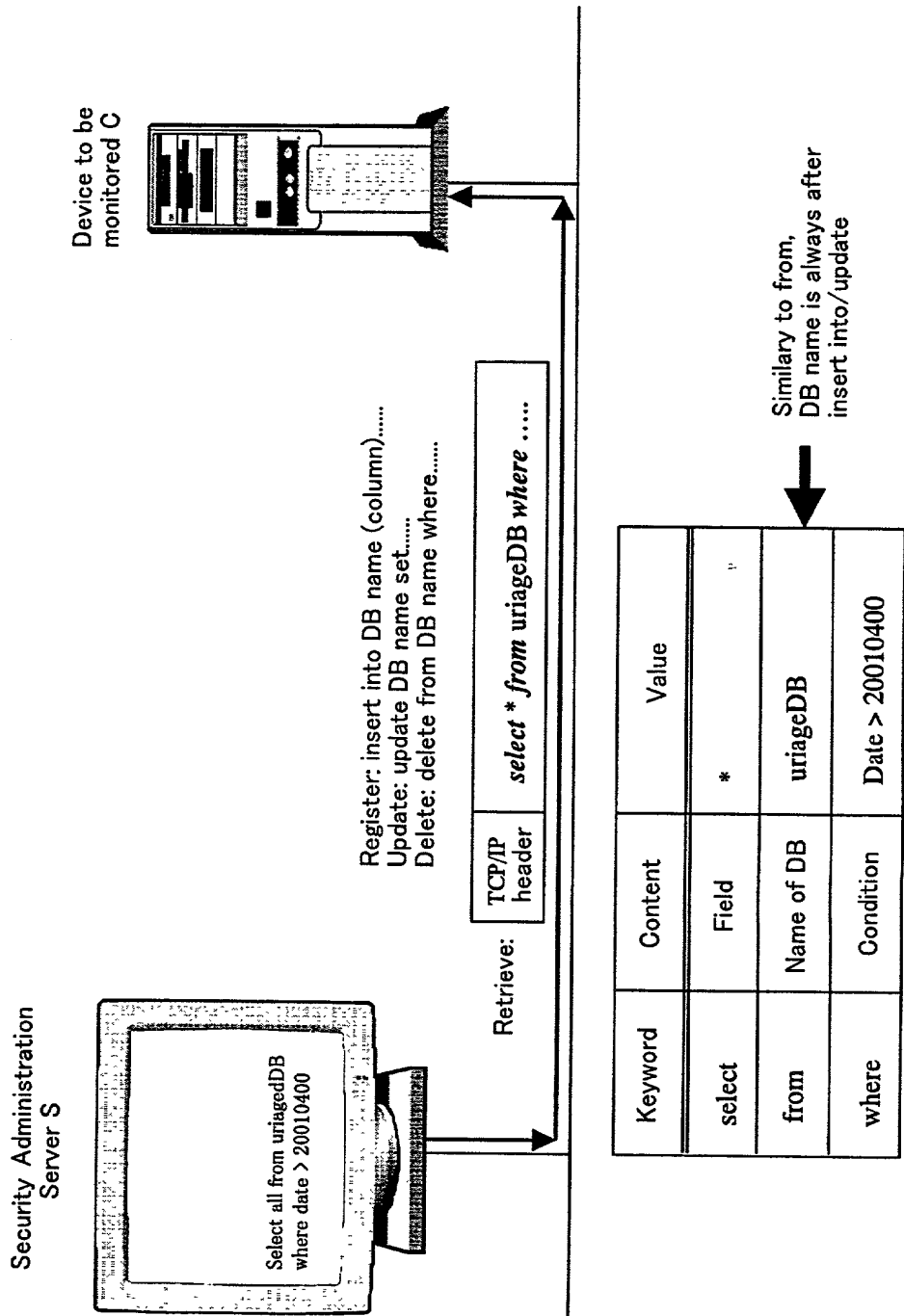


FIG. 22